

American Electronics Association

Representing the U.S. electronics, software and information technology industries

AEA

WWW Address: <http://www.aeanet.org>

5201 Great America Parkway, Suite 520, Santa Clara, CA 95054 Telephone: 408-987-4200 Fax: 408-970-8565

Mailing Address: P.O. Box 54990, Santa Clara, CA 95056-0990

1225 Eye Street, N.W., Suite 950, Washington, D.C. 20005 Telephone: 202-682-9110 Fax: 202-682-9111

#45
pg 1 of 6

February 13, 1997

Honorable William A. Reinsch
Under Secretary of Commerce for Export Administration
Bureau of Export Administration
US Department of Commerce
14th Street & Pennsylvania Ave., NW
Washington, DC 20230

Dear Bill:

The American Electronics Association appreciates this opportunity to comment on the Administration's December 30 implementation of its October 30 policy on key recovery encryption export policy. The AEA represents more than 3000 American high technology companies which in turn represent virtually every encryption business interest -- from computer and telecommunications hardware and software, to internetworking equipment and services -- and every point of view on this controversial issue.

It is with this breadth of involvement that our members convey serious doubts about the viability of the Administration's proposal and continue to seek ways to alter the direction of this policy.

As you know, several AEA members have chosen to work within the parameters given industry to attempt to devise key recovery features in our encryption products as a condition for being able to export stronger encryption products than was allowed under current law. Other AEA members continue to assert the unworkability of key recovery, citing technical and logistical vulnerabilities as well as fatal competitive disadvantage in the face of foreign encryption products not subject to the same restrictions. Rather than restate the numerous concerns that we expressed about the October 1 policy announcement, we have attached our comments as delivered to the White House shortly thereafter.

Overall, we continue to believe that dialogue with the Administration may result in a policy that acknowledges the widespread foreign availability -- and inherent uncontrollability -- of robust encryption far stronger than 56 bit key length. Legislative initiatives on Capitol Hill are attempting to engage a policy that addresses that very point and we anticipate giving those initiatives serious attention as the 105th Congress progresses.

Understanding that this complex policy debate requires time and resources to achieve major shifts in direction, we would like to offer interim comments designed to address several of the immediate problems in the policy as found in the implementing regulation published in interim form on December 30.



Specific Comments

LICENSE PROCESSING TIMES. AEA has long supported the transfer in jurisdiction for export licensing of cryptographic products from the State to the Commerce Department. In doing so, we have placed a high premium on ensuring that license processing times are faster than under the State Department regime.

Unfortunately, it appears that license turnaround times are taking much longer with the transfer in jurisdiction to the Commerce Department. Initial indications are that some license applications that were being turned around by the Department of State in as little as 5 days are now taking 30 to 40 days to approve.

Industry representatives have been repeatedly assured by members of the Administration that the new regulations would not make the approval of encryption exports any more difficult than it was at the State Department. However, the increases in license processing times that have emerged since the jurisdiction transfer are steering a course in the opposite direction. Companies that produce encryption products are fast-moving and must be able to obtain timely export approval in order to compete in the global marketplace. Compared to the few days it routinely took to process applications at the State Department, processing times of 30 days or more represent delays that U.S. companies cannot afford.

In part, the cause of such delays seems attributable to the fact that agencies and individuals that had not previously been involved in encryption licensing are now reviewing applications items and technology with which they are not familiar. This part of the problem would seem likely to diminish over time.

A much more serious problem, however, is the fact that all applications for encryption export licenses now must go through a lengthy interagency review process. Under the Export Administration Regulations (EAR), as amended, the Departments of Defense, Energy, Justice, State, and the Arms Control and Disarmament Agency (ACDA) have the authority to review all license applications for encryption exports submitted to the BXA.

However, Energy, ACDA, Defense and State do not have a significant interest in most exports of commercial encryption. Review by these agencies contributes to unnecessary delays in the consideration of license applications for encryption items.

AEA recommends that the Administration act immediately to ensure quick license processing times for encryption exports. Specifically, those agencies that do not have a significant interest in commercial encryption exports should grant a delegation of authority to the BXA. Section 750.3 of the EAR provides:

"Though these agencies have the authority to review any license application, they may determine that they do not need to review certain types of license applications. In these instances, the agency will provide BXA with a Delegation of Authority to process those applications without review by that particular agency."

For the vast majority of applications for commercial encryption exports, the delegations would eliminate unnecessary steps and should significantly speed the processing of such license applications.

LACK OF END-USER AND END-USE PROVISIONS. While commercial encryption was under the jurisdiction of the State Department, the government demonstrated a willingness to allow the export of encryption products that would normally be controlled (e.g. non-recovery 56-bit DES) to certain end users and/or for certain end-uses. For example, overseas banks and financial institutions have been allowed to receive such items provided their use is limited to protecting the security of financial transactions. Similarly, U.S. companies have been allowed to export strong encryption products to the foreign subsidiaries of those companies in order to protect their internal corporate communications.

AEA notes with appreciation that previously granted State Department licenses, distribution arrangements, or other export approvals will be continued under the Commerce Department regime. In this context, AEA assumes the Commerce Department will continue the State Department's practice of according preferential treatment to certain commercial exports of encryption. This includes extending export approvals to non key recovery encryption of any strength that is to be exported for financial end uses or internal use by U.S. corporations. AEA strongly recommends that this treatment be expanded to include consideration of all commercial end uses/users in the export approval process, based on customer reliability, specific end use and country guidelines. Such expanded treatment, while not requiring amendment of the interim regulations, should nevertheless become an integral part of the Commerce Department's administrative practice for handling encryption exports.

OTHER. AEA also urges the Department of Commerce to make the following adjustments to the current encryption export regulations:

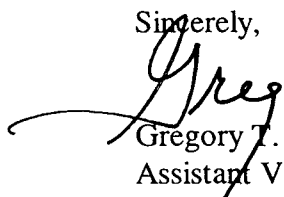
- A 40 bit hardware exception must be made equivalent to the 40 bit software mass market exception.
- Products with cryptography should be subject to traditional foreign availability assessments as are all other technologies under Commerce jurisdiction. Not allowing for foreign availability determinations undermines a fundamental and long standing principle under the 'dual use' export control regime.
- Allow for reexport of foreign made encryption, by reinstating the de minimis US content exception.
- ITAR license exemptions which covered parts and spare under \$500 were lost in the transition to Commerce and should be reinstated under license exception LVS.

- ITAR exemptions covering temporary exports to subsidiaries for assembly and subsequent return to the US also were lost in the Commerce transition and should be reinstated under license exception TMP.
- Allow the export of systems that have cryptographic Applications Program Interfaces (APIs) to at least the level that is permitted to be exported.
- While the elimination of record keeping requirements under the personal use exemption was a positive development which we applaud, the scope of the exemption restricts the countries that are eligible for use of the exception beyond restrictions that were present in the ITAR. License exception TMP should be revised to permit eligibility of temporary encryption exports for personal use to all countries other than embargoed destinations.
- Continued effort must be made by the Commerce Department to further liberalize export controls on cryptography to provide relief for mass market products with cryptography.

Beyond the recommendation stated above concerning the need for parity between the export treatment of 40 bit software vs hardware products, the need for fair and equitable export treatment between hardware and software products above 40 bit cryptography must also be reflected in any liberalization policy.

Thank you for the opportunity to comment on the Administration's encryption policy.

Sincerely,



Gregory T. Garcia
Assistant Vice President, Trade Regulation

attachment

AMERICAN ELECTRONICS ASSOCIATION



STATEMENT BY THE AMERICAN ELECTRONICS ASSOCIATION ON THE CLINTON ADMINISTRATION ENCRYPTION PROPOSAL

The Clinton Administration's October 1 encryption initiative takes a step toward achieving AEA's goal of export control reform for cryptographic exports. Positive elements of the announcement include the transfer of licensing jurisdiction to the Commerce Department as well as a recognition of the need to export cryptographic products with key lengths greater than 40 bits.

A number of serious issues are raised by the announcement, however. First, the binding between key recovery and 56-bit encryption exports cuts against the grain of a market-driven approach and ignores the need for immediate liberalization of 56-bit encryption without any contingencies. Key recovery systems only stand a chance of gaining wide acceptance if they meet the commercial demands of the global marketplace. Indeed, foreign customers may decide not to deploy US encryption products at all, for fear that the robust systems in which they have invested must, after the two year transition, be accompanied by potentially undesirable key recovery features.

Second, the key recovery binding could result in unequal treatment of exporters. Large exporters are likely to be better positioned than small exporters to attempt compliance with key recovery requirements.

Third, the AEA views with concern the unprecedented use of Federal law enforcement as a statutory basis for export controls. The Administration intends to facilitate key recovery through legislation, and we intend to ensure that such legislation addresses the above issues in a way that satisfies the IT industry and its users.

The Administration's initiative does not address two other important bases for export control reform: 1) the inability to control effectively non-key recovery encryption products that have been on the global market and will be more so after the two year period; and 2) the lack of marketability and competitiveness of U.S. cryptographic products with key recovery versus foreign non key recovery products. Industry's ability to address the marketability and competitiveness challenges are contingent on satisfying key recovery criteria that are unproven and may never gain acceptance in the global marketplace. Nor is it clear that key recovery solutions are applicable to all uses of encryption. The elusive prospect of a globally implemented standard leads us to conclude that we cannot remain competitive if our only permissible exports above 40 bits are key recovery-based.

But a post-transition *recontrol* of non key recovery encryption is unworkable and ignores the global diffusion of powerful, unregulated encryption. After the two year transition, non key recovery encryption products at 56 bits and above will have saturated many markets worldwide and made significant inroads in less developed markets. Recontrolling these products could undermine established business relationships (such as those formed around non key recovery products previously licensed by the State Department) and commercial security with no apparent national security or law enforcement gain.



Conclusion and Recommendations

AEA is hopeful the Administration's announcement will lead to real progress in promoting both US competitiveness in the global cryptography market and U.S. national security. To get to that point, the implementation of this program must adhere to the following essential principles:

- Immediate transfer of licensing jurisdiction from State to Commerce, in a manner that fosters faster, more efficient processing than under the State Department regime;
- Prohibition against government mandates of specific key recovery criteria;
- Prohibition against domestic use restrictions;
- Assurances that companies which have made good faith efforts to develop key recovery in their encryption products will be able to continue to support customers using non-key recovery products;
- Assurances that encryption products providing alternative means of access will be eligible for the same licensing treatment given to key recovery products.
- Greater ability to export both hardware and software interfaces;
- Use of the Administration's "formal mechanism" for implementation review to assess at the end of the two-year transition the foreign availability, under current Commerce Department procedures, of non-key recovery 56-bit encryption and above; and
- Recognition that, in the end, the encryption problem must be solved by fighting technology with technology rather than through regulation.

October 1996